UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/993,450	11/06/2001	Massimo DiPierro	089326-0101	8018

27433 7590 07/06/2005

FOLEY & LARDNER
321 NORTH CLARK STREET
SUITE 2800
CHICAGO, IL 60610-4764

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/993,450	DIPIERRO, MASSIMO	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *see Office action*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The Information Disclosure Statements filed 06 November 2001, 09 May 2002, 27 June 2003, and 16 December 2003 have been considered by the Examiner.

Specification

2. The disclosure is objected to because of the following informalities:

The specification appears to contain minor typographical and other errors. For example, in paragraph 0029, line 7, it appears that in the phrase "Yet another situation such situation", the words "such situation" should be deleted. In paragraph 0058, there is a reference to "application 601"; however, 601 was previously used to refer to the operating system and hardware side. Further, in paragraph 0145, there is a blank line that appears to be reserved for file names in the CD appendix.

The above is not an exhaustive list. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Appropriate correction is required.

Claim Objections

3. Claims 7 and 12 are objected to because of the following informalities:

In Claim 7, line 3, it appears that "inputing" is intended to read "inputting". In Claim 12, line 7, it appears that "entier" is intended to read "entire".

Appropriate correction is required.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 12-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Although the claims recite "A machine readable medium comprising computer code", the term "machine readable medium" is much broader than a "computer readable medium", and encompasses non-statutory embodiments. Further, the language of the specification raises a question as to whether the claim is directed merely to an abstract idea that is not tied to a technological art, environment, or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101. Specifically, in paragraph 0027, the specification states that the file storage medium can include paper or any other "media capable of receiving data for storage". This renders the claims non-statutory. See MPEP § 2106 IV.B.

6. To expedite a complete examination of the instant application, the claims rejected under 35 U.S.C. 101 above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the statutory classes of invention.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 6-11, 17, 20, and 21 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 6 and 11 recite the limitation "the user signature". There is insufficient antecedent basis for this limitation in the claims.

Claim 7 recites the limitation "the temporary, encrypted file". There is insufficient antecedent basis for this limitation in the claims, although it appears that this could refer to the "encrypted, temporary copy of the file" recited earlier in the claim.

Claim 8 recites the limitation "the file". It is unclear whether this refers to the file first recited in Claim 1, or to the "temporary, encrypted file" of Claim 7. This renders the claim indefinite. For purposes of interpreting the prior art, it is assumed that "the file" refers to the file of Claim 1. Further, Claim 8 recites the limitation "the temporary, encrypted file". There is insufficient antecedent basis for this limitation in the claims,

although it appears that this could refer to the "encrypted, temporary copy of the file" recited in Claim 7.

Claim 9 recites "The method of claim 9". This renders the claim indefinite, as all the limitations incorporated by the claim are not clear. For purposes of interpreting the prior art, it has been assumed that Claim 9 is intended to depend from Claim 7. Further, Claim 9 recites the limitation "the temporary, encrypted file". There is insufficient antecedent basis for this limitation in the claims, although it appears that this could refer to the "encrypted, temporary copy of the file" recited in Claim 7. Additionally, Claim 9 recites the limitation "the file". It is unclear whether this refers to the file first recited in Claim 1, to the "temporary, encrypted file" of Claim 7, or to the "encrypted, temporary file" recited earlier in Claim 9. This renders the claim indefinite. For purposes of interpreting the prior art, it is assumed that "the file" refers to the file of Claim 1.

Claim 10 is rejected due to its dependence on rejected Claim 7.

Claim 17 recites the limitation "such that encryption, decryption, and authentication a transparent to a source code programmer". This limitation is generally vague and unclear, which renders the claim indefinite.

Claim 20 recites the limitations "the encrypted, temporary file" and "the temporary, encrypted file". There is insufficient antecedent basis for this limitation in the claims, although it appears that this could refer to the "temporary, encrypted copy of the file" recited earlier in the claim.

Claim 21 recites the limitation "adding the encrypted digital signature and the encrypted user signature to the temporary copy to authenticate it". It is unclear whether

"it" refers to the encrypted digital signature, the encrypted user signature, or the temporary copy, although it appears that "it" was intended to refer to the temporary copy.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1-6, 12, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, *Applied Cryptography*.

In reference to Claim 1, Schneier discloses a method that includes calculating and storing a digital signature for a file (see page 30, section 2.4, "One-Way Hash Functions", where a hash can be created by pre-imaging a file and XORing strings of bits together). Schneier further discloses encrypting a file and performing a file input-output operation on a proper subset of the file in a manner that permits the input-output operation without needing to decrypt the entire file (see page 190, noting the first full paragraph where ECB mode is recommended for encryption of database records). Therefore, it would have been obvious to combine the digital signature and encryption as taught by Schneier, in order to gain the integrity of digital signatures (see page 35)

and the advantages of electronic codebook mode block encryption to allow blocks to be decrypted independently (see page 190).

In reference to Claims 2 and 3, Schneier further discloses inputting a data subset and decrypting the data subset (see page 190). Further, it would have been obvious to one of ordinary skill in the art at the time the invention was made to update the digital signature after changing a file, so that the signature correctly reflects the contents of the file.

In reference to Claim 4, Schneier further discloses encrypting a data subset to be written and writing the encrypted data (see page 190).

In reference to Claims 5 and 6, Schneier further discloses authenticating a file using signatures (see page 35).

In reference to Claim 12, Schneier discloses reading from and writing to an encrypted file without requiring decryption of the entire file (see page 190, noting the first full paragraph where ECB mode is recommended for encryption of database records). Schneier further discloses calculating and storing a digital signature for a file (see page 30, section 2.4, "One-Way Hash Functions", where a hash can be created by pre-imaging a file and XORing strings of bits together). Therefore, it would have been obvious to combine the digital signature and encryption as taught by Schneier, in order to gain the integrity of digital signatures (see page 35) and the advantages of electronic codebook mode block encryption to allow blocks to be decrypted independently (see page 190).

In reference to Claim 13, Schneier further discloses discloses authenticating a file using signatures (see page 35).

11. Claims 7-11 and 14-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Borman et al, US Patent 5437026.

In reference to Claim 7, Schneier discloses everything as applied above to Claim 1. Schneier further discloses inputting a data subset and decrypting the data subset (see page 190). However, Schneier does not explicitly disclose inputting the subset from a temporary copy of the file. Borman discloses a method including creating a duplicate, temporary copy of a file (see column 2, lines 12-30). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the creation of a temporary file copy, in order to allow for data recovery in the event of a system failure or abnormal termination (see Borman, column 1, lines 35-45; column 2, lines 14-24).

In reference to Claims 8 and 9, Schneier further discloses encrypting a data subset to be written and writing the encrypted data (see page 190). Further, it would have been obvious to one of ordinary skill in the art at the time the invention was made to update the digital signature after changing a file, so that the signature correctly reflects the contents of the file.

In reference to Claims 10 and 11, Schneier further discloses authenticating a file using signatures (see page 35).

In reference to Claim 14, Schneier discloses everything as applied above to Claim 13. However, Schneier does not explicitly disclose inputting the subset from a temporary copy of the file. Borman discloses a method including creating a duplicate, temporary copy of a file (see column 2, lines 12-30). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the creation of a temporary file copy, in order to allow for data recovery in the event of a system failure or abnormal termination (see Borman, column 1, lines 35-45; column 2, lines 14-24).

In reference to Claim 15, Schneier further discloses using a symmetric, invertible function to implement the digital signature (see page 30, section 2.4, "One-Way Hash Functions", where a hash can be created by pre-imaging a file and XORing strings of bits together, noting that XOR is symmetric and invertible).

In reference to Claims 16-18, Schneier further discloses authenticating a file using signatures (see page 35).

In reference to Claim 19, Schneier further discloses applying functions to a database (see page 190).

In reference to Claim 20, Schneier discloses a method that includes storing sensitive data in an encrypted file, decrypting a subset of the file when performing read and write operations, and encrypting a data subset to be written and writing the encrypted data (see page 190, noting the first full paragraph where ECB mode is recommended for encryption of database records). Schneier further discloses

calculating and storing a digital signature for a file (see page 30, section 2.4, "One-Way Hash Functions", where a hash can be created by pre-imaging a file and XORing strings of bits together). Therefore, it would have been obvious to combine the digital signature and encryption as taught by Schneier, in order to gain the integrity of digital signatures (see page 35) and the advantages of electronic codebook mode block encryption to allow blocks to be decrypted independently (see page 190). Further, it would have been obvious to one of ordinary skill in the art at the time the invention was made to update the digital signature after changing a file, so that the signature correctly reflects the contents of the file. However, Schneier does not explicitly disclose inputting the subset from a temporary copy of the file. Borman discloses a method including creating a duplicate, temporary copy of a file and updating the file with the temporary copy when closing the file (see column 2, lines 12-30). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the creation of a temporary file copy, in order to allow for data recovery in the event of a system failure or abnormal termination (see Borman, column 1, lines 35-45; column 2, lines 14-24).

In reference to Claim 21, Schneier discloses a method that includes creating and encrypting a file containing sensitive data, and performing a file input-output operation on a proper subset of the file without needing to decrypt the entire file, where the operation includes decrypting a subset of the file when performing read and write operations, and encrypting a data subset to be written and writing the encrypted data (see page 190, noting the first full paragraph where ECB mode is recommended for

encryption of database records). Schneier further discloses calculating and storing a digital signature for a file (see page 30, section 2.4, "One-Way Hash Functions", where a hash can be created by pre-imaging a file and XORing strings of bits together). Therefore, it would have been obvious to combine the digital signature and encryption as taught by Schneier, in order to gain the integrity of digital signatures (see page 35) and the advantages of electronic codebook mode block encryption to allow blocks to be decrypted independently (see page 190). Further, it would have been obvious to one of ordinary skill in the art at the time the invention was made to update the digital signature after changing a file, so that the signature correctly reflects the contents of the file. However, Schneier does not explicitly disclose creating a temporary copy of the file. Borman discloses a method including creating a duplicate, temporary copy of a file and updating the file with the temporary copy when closing the file (see column 2, lines 12-30). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the creation of a temporary file copy, in order to allow for data recovery in the event of a system failure or abnormal termination (see Borman, column 1, lines 35-45; column 2, lines 14-24).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-

3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AAD
zad

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100